Strategy Research Project

INFORMATION OPERATIONS: THE MILITARY'S ROLE IN GAINING INFORMATION SUPERIORITY

BY

COLONEL MICHAEL J. DOMINIQUE
United States Army

USAWC CLASS OF 2009

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
17-03-2009	Strategy Research Project	

4. TITLE AND SUBTITLE

Information Operations: The Military's Role in Gaining Information Superiority

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Michael J. Dominique

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Philip M. Evans
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The use of Information Operations (IO) as an integration process is paramount in today's information environment to achieve information superiority. If it is true that information is an element of national power, then IO is the U.S. military's contribution to supporting the national information effort. Formalization of IO into the U.S. Army structure began in 1999 with the establishment of IO as a functional area. Over the past ten years, the U.S. military has witnessed continued refinement and evolution of the IO definition and employment, improved integration of core, supporting, and related IO elements into military operations, and the emergence of a variety of IO enablers. The intent of this project is to provide a consolidated look at IO in its current state, present some thoughts and recommendations from an IO practitioner regarding IO and the other capabilities that effect the information environment, and address some of the points of confusion regarding IO within the military. Six recommendations are provided on how the U.S., specifically the military, can improve the IO structure and its employment process.

15. SUBJECT TERMS

Information Engagement, Information Element of Power, Psychological Operations, Strategic Communications

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	38	

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS: THE MILITARY'S ROLE IN GAINING INFORMATION SUPERIORITY

by

Colonel Michael J. Dominique
United States Army

Colonel Philip M. Evans
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Michael J. Dominique

TITLE: Information Operations: The Military's Role in Gaining Information Superiority

FORMAT: Strategy Research Project

DATE: 17 March 2009 WORD COUNT: 7842 PAGES: 38

KEY TERMS: Information Engagement, Information Element of Power, Psychological Operations, Strategic Communications

CLASSIFICATION: Unclassified

The use of Information Operations (IO) as an integration process is paramount in today's information environment to achieve information superiority. If it is true that information is an element of national power, then IO is the U.S. military's contribution to supporting the national information effort. Formalization of IO into the U.S. Army structure began in 1999 with the establishment of IO as a functional area. Over the past ten years, the U.S. military has witnessed continued refinement and evolution of the IO definition and employment, improved integration of core, supporting, and related IO elements into military operations, and the emergence of a variety of IO enablers. The intent of this project is to provide a consolidated look at IO in its current state, present some thoughts and recommendations from an IO practitioner regarding IO and the other capabilities that effect the information environment, and address some of the points of confusion regarding IO within the military. Six recommendations are provided on how the U.S., specifically the military, can improve the IO structure and its employment process.

INFORMATION OPERATIONS: THE MILITARY'S ROLE IN GAINING INFORMATION SUPERIORITY

In this modern age of technology, the information element of power is seen by many as the solution to a multitude of problems, but it is not the 'holy grail' to solve all of them. Just as the U.S. national leadership has understood the importance of information as an element of power, our military leadership has fully embraced information operations as a combat multiplier. With all the attention given to the information element of power, the establishment of Information Operations (IO) as a formal and permanent capability within the military structure, and continuous refinement of IO employment techniques, why is the U.S. losing the battle for information superiority? Are we indeed losing the IO war as so many state we are?

U.S. Joint doctrine defines Information superiority as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying any adversary's ability to do the same."[1] Utilizing this definition one could conclude that we have indeed maintained information superiority overall. Granted, this superiority has not been continuous, but our adversaries have only achieved temporary successes. The intent of this project is to provide a consolidated look at IO in its current state, present some thoughts and recommendations from an IO practitioner regarding IO and the other capabilities that effect the information environment, and address some of the points of confusion regarding IO within the military.

Information Operations Defined

Joint Publication (JP) 3-13, *Information Operations*, describes IO as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC) and operations security (OPSEC) in concert with specific supporting and relating capabilities to influence, disrupt, or usurp adversarial human and automated decision making while protecting our own."[2] This process does not replace the core, specified supporting or related capabilities but rather enhances their individual effects through synchronizing their efforts. Defining information operations and effectively employing it is a different matter. Integrating the military tool of IO with strategic communication and public diplomacy presents a host of concerns to include legal challenges, perceptions, and communication technology.

The act of informing is a way to influence a specific target audience but informing does not mean that the target audience will accept the information regardless of its truthfulness. Misunderstanding IO and confusing the process with the action of influencing are just some of the challenges facing the IO practitioner. The ability to balance and coordinate the information flow, presenting the target audience with an environment where the information is supported by action is key. Different target audiences require different capability applications. Use of the organic capabilities to shape, inform and influence in a concerted effort requires a synchronized effort such as depicted in figure 1, a conceptual depiction of an IO concept of support for the Iraqi information environment.

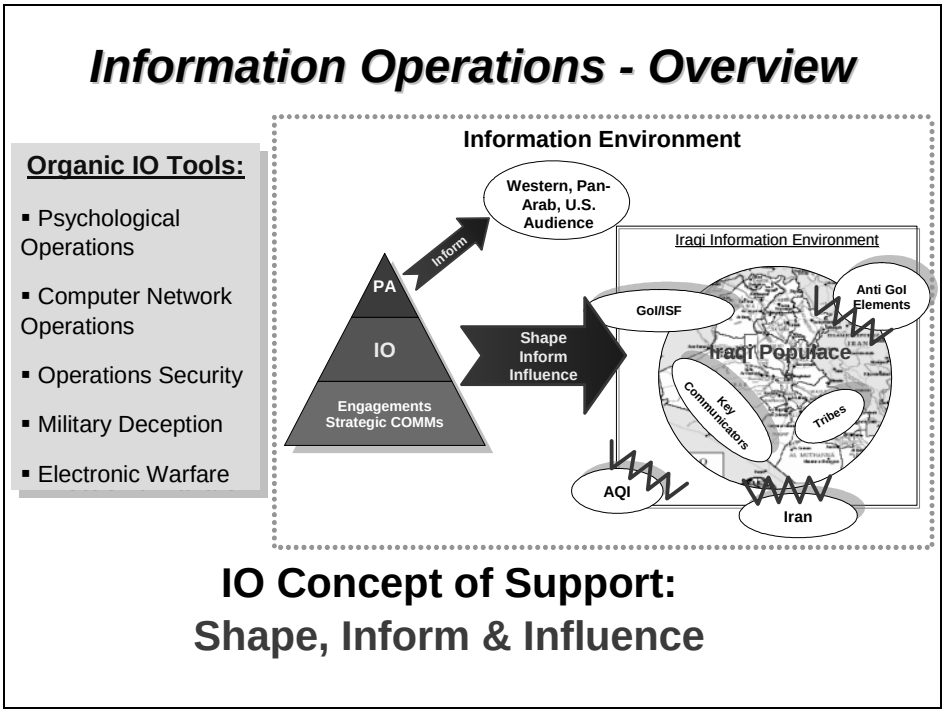

Figure 1. IO Concept of Support[3]

As stated earlier, there are some who consider information an element of national power and believe that the U.S. should increase its reliance on information as an instrument of national power. If information is an element of national power, then IO is the military's contribution to support the national information effort. *The 2006 National Security Strategy* states "democracy offers freedom of speech, independent media, and the marketplace of idea, which can expose and discredit falsehoods, prejudices, and dishonest propaganda."[4] The challenge becomes providing factual information to an audience that is swayed by misinformation and a concerted effort by adversaries to mislead. IO provides our military and government a capability to use information as a weapon system but balancing the military capability with the strategic communication can be confusing. Our own doctrine terminology adds to the confusion of how to leverage information, what the military refers to, as a weapon system. The U.S.

military's use of information is focused on an adversary to disrupt their activities while influencing conduit targets from supporting adversaries. Protection of our own information assets while preventing adversaries from negatively influencing neutral audiences removes an invaluable resource from an enemy's arsenal.

Our adversaries are not held by the same legal and ethical reporting requirements that U.S. agencies are expected to uphold. The challenge is when the media and public cannot distinguish between information, misinformation or even disinformation. IO is the key tool which the military can use to counter misinformation and disinformation or use its capabilities to influence, disrupt or usurp an adversary's decision-making cycle. The hesitation for U.S. agencies to market our own actions to neutral or friendly audiences puts us at a distinct disadvantage. How does the U.S. "sell" the truth or market its intentions to a target audience that is convinced that all our actions have ulterior motives or that we are attempting to mislead them? Attempts to market our efforts or to promote success are routinely seen with skepticism and concern by U.S. and foreign audiences.

Background on U.S. Information Operations

Although various elements of IO have been prevalent throughout the history of warfare it was during World War I that organized efforts emerged to harness the power of information. England's control of the trans-Atlantic cable gave the Allies the advantage in information control. The U.S. government's creation of the Committee on Public Information (CPI) gave the U.S. an instrument to not only counter propaganda but also a venue to influence international and national audiences. Utilizing strategic communication in its current form, the CPI "understood the task required to mobilize

disparate elements of the population behind the war effort and the critical role information played...."[5] As WWI progressed; the need for an increased air capability became evident. The U.S.'s Aircraft Production Board developed a program to garner support and influence the political structure to assure approval of its efforts. Efforts included direct engagement with various American media outlets. The end result was a presidential signature to provide the required funds and support.[6]

During WWII the U.S. government instituted the Office of War Information (OWI) to aid in focusing information. This information effort was vital to the U.S.'s war effort to keep up moral of the American people and to bolster our allies. Although the U.S.'s propaganda effort was directed at the Axis powers, the development of programs to support the war effort was clearly directed at the American people. The purchase of war bonds and rationing programs, the movie industry's portrayal of the brave American Soldier and the villainous enemy, and the short news clips highlighting U.S. victories were all efforts to influence and inform the U.S. population. These efforts were not IO but were forms of strategic communication, so how did the U.S. employ IO in WWII? The "loose lips sinks ships" OPSEC programs, vast deception efforts, propaganda, and numerous other programs focused on the Axis leadership and enemy or neutral populations in a military effort to inform, influence and disrupt.

The CPI, OWI and the Office of Strategic Influence have all been the government’s attempt to focus and synchronize the element of information but each has out lived its usefulness or been terminated due to public outcry. Confusion regarding IO, strategic communication or simple efforts to inform seems commonplace. Military doctrine says the military commander can use IO to destroy, disrupt, degrade, deny,

deceive, exploit, influence, protect, detect, restore, and respond.[7] Defining information terminology in general terms adds to the confusion. A simple comparison of the definitions of propaganda, IE, and strategic communication shows the undefined boundaries (see figure 2). The simple act of informing could be seen as an IO capability and factual informing, in a timely manner, is a powerful weapon.

The Importance of Information

The importance of information is well understood by both our leadership and the adversaries we face on the modern, complex battlefield. Modern information technology provides immediate and up to date information but this overwhelming information requires analysis, assessment, and protection. The Department of Defense (DoD) has dedicated large amounts of resources to protect our computer networks, to inform and influence target audiences, to synchronize various information efforts to achieve a desired end state, and to disrupt adversarial decision making cycles through a multitude of methods. With all these dedicated resources to promote information as a tool to influence, it is the denial of information that aids the disruption of an adversary's effective decision-making. The question remains, with all the information technology, the dedicated resources, and the leadership guidance, why is the information effort so disjointed? The development of strategic communications, information engagement (IE), and the use of public media by adversaries has resulted in a wide variety of perspectives on what defines the information element of power, how the military's role of IO fits in the overall information effort, and the best method to employ information capabilities.

Propaganda (JP 1-02)	Information Engagement (FM 3-0)	Strategic Communication (JP 1-02)
Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly.	The integrated employment of public affairs to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. Government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and, leader and Soldier engagements to support both efforts.	Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power.

Figure 2. Information Terminology[8]

The Contemporary Information Operations Environment

For the military, the institution of an IO doctrine, a career force, and a formal training program has been a slow and painful process. Each service has developed its own capability in order to meet the DoD Directive to the Chairman of the Joint Chiefs of Staff to "provide oversight to ensure that the U.S. Armed Forces maintain the capabilities and capacity so that they are as effective in irregular warfare as they are in traditional warfare."[9] Today's shift from traditional warfare to irregular warfare increases the need of military information capabilities and increases the need to ensure that military efforts are synchronized with U.S. civilian information agencies. Although the military's focus has been on the IO process, the challenges of strategic communication development are closely linked.

To best employ IO one must understand IO, its elements and how they all "fit"

together. The core capabilities of IO are EW, CNO, PSYOP, MILDEC and OPSEC but other capabilities that are related or supporting can also have an impact on the information environment. It is IO that is "primarily concerned with affecting decisions and decision making processes, while at the same time defending friendly decision making processes."[10] IO serves as the process that integrates and focuses all IO capabilities to achieve a synchronized effort while making maximum use of the success of the related capabilities such as public affairs (PA), civil-military operations (CMO), and defense support to public diplomacy (DSPD).

U.S. Information Operations – Core Elements

IO success is the ability to focus and synchronize the distinct efforts of various information tools to achieve the commander's desired effect. Observations of various military and civilian organizations who have scrutinized the employment of IO stated that the IO process is not understood by some civilian and military leadership and that there is a misconception that IO is just the coordinated application of PSYOP, CMO, and PA.[11] As stipulated in its definition, IO is the integrated employment of capabilities, not a single capability in its own right; IO is a means to enhance our efforts through a synchronized effort that supports and compliments its core, supporting, and related capabilities.

Psychological Operations (PSYOP). JP 3-13 states that PSYOP's purpose is to "induce or reinforce foreign attitudes and behavior favorable to the originator's objectives".[12] Recent military operations in both Iraq and Afghanistan have seen a resurgence in the usefulness of PSYOP in influencing foreign audiences, but along with this success there has been a growing confusion regarding the relationship between

PSYOP and IO. With the introduction of IO as a capability to achieve information superiority, it is natural for PSYOP to assume the lead role in influencing adversarial and neutral populations. By the time the IO became a formal functional area the PSYOP community had already developed a standardized approval process, developed manning and training programs, and documented techniques, tactics and procedures (TTPs). It is not surprising that leadership and the fledging IO community embraced the PSYOP TTPs and focused primarily on PSYOP as the key source to influence. PSYOP is not IO; rather PSYOP is one of the information tools to achieve the IO objective. PSYOP is a tool of the IO process, with a distinct mission of influencing foreign audiences. It also provides a means, as the IO definition describes, to influence, disrupt, or usurp adversarial human decision making through conduit targets. While the target of PSYOP is the foreign audience, the second and third order effects can and normally do influence, disrupt or usurp an adversary's decision making.

Concern about the U.S. government's potential to manipulate the U.S. population resulted in legislative steps to prevent abuse of this powerful influencing tool. In a 2007 article in *Parameters*, Professor Dennis Murphy pointed out that "Congress passed the Smith-Mundt Act in 1948, recognizing the importance of marshalling US cultural and information outreach efforts in support of national engagement in what was coming to be called the 'Cold War'. But it carefully stipulated that such programs, fashioned for foreign audiences, could not be disseminated at home."[13] The PSYOP community's ability to inform foreign audiences through a wide variety of information venues that includes satellite TV, radio, leaflets, and face-to-face engagements has provided an important ability to remove support from an adversary. As PSYOP continues to improve

its dissemination means, the concern that PSYOP messaging could also potentially influence Americans increases.

Many times the ability to inform a target audience of factual events is the best way to influence them. Today's target audience has access to international media, is probably familiar with the engagements conducted by U.S. representatives, and is personally connected to the events as they occur so any type of misleading messaging will be met with immediate skepticism. If there is a contradiction between the PSYOP products and other sources that the target sees as legitimate, credibility is lost. Without credibility, the PSYOP messaging is counterproductive. IO aids in maintaining the PSYOP credibility through its integration efforts, facilitating the messages that are at times common throughout the information effort. The stigma of PSYOP as a capability that is designed to mislead or unduly influence is a false perception. Legal constraints and cultural misunderstandings about the role of PSYOP in the overall information effort continue to add to the confusion of how to integrate information effectively. In today's media environment, the challenge of restricting messaging only to a foreign audience is difficult.

The recent challenges concerning the use of foreign media to influence specific target audiences clearly demonstrates the legal and ethical issues when faced with how to provide factual information in foreign media. The close coordination between PA and PSYOP to counter adversarial misinformation or disinformation is a purpose of the IO cell.[14] The capabilities and expertise of the PSYOP community provides the means to inform foreign audiences through a wide menu of communication venues. The 2005 revelation that the U.S. military was involved in the paid placement of news reports

demonstrated a concern regarding the U.S. government's role in influencing audiences both foreign and internal. Although the stories placed in Iraqi newspapers were accepted as truthful, they were considered to only "present one side of events and omit information that might reflect poorly on the U.S. or Iraqi governments."[15] Immediately there were accusations of propaganda and a concern about the information spreading to domestic media. Although the organization that engineered the effort was not a PSYOP organization, the event highlights the concern of multiple organizations attempting to influence a foreign audience. It also highlights the issue of attempting to influence a foreign audience through media outlets.

Accusations that IO routinely takes credit for PSYOP products and success could be a direct result of the IO community's attempt to inform its leadership of ongoing information efforts. Most leadership desire quantitative data to demonstrate progress and the PSYOP community's efforts are easily packaged for briefing ease. Briefing the other capabilities and showing quantitative progress is at times difficult. The IO community must learn to expand their own planning efforts to demonstrate to military leadership the progress and effectiveness of the overall effort rather than just the PSYOP effort.

The IO community must focus on the overall process, balancing PSYOP and the other information tools. Referring to IO products in the form of handbills, influence products, or other message dissemination just adds to the confusion. The PSYOP community provides a great amount of resources to the information effort to include expertise regarding the culture and various target audiences, resources to disseminate themes and messages, manpower, and a means to provide effectiveness of

assessments. With the PSYOP community's assistance, IO must refine its ability integrate PSYOP into the overall information effort. The IO community must be cautious not to assume the role of PSYOP; the mission of influencing foreign audiences must be retained by the subject matter experts. IO must focus on integration and should seek out the means to support PYSOP by ensuring that all the capabilities' efforts are mutually supporting not counterproductive.

Computer Network Operations (CNO). As a core element of IO, CNO serves as a means of defending information and disrupting decision-making cycles by preventing adversaries from gaining a distinct advantage through their computers actions. The use of the Internet by the military for communication, information acquisition, and information dissemination serves as a double-edged sword. The use of the Internet serves as a force multiplier but it also requires protection. The role of the Internet is key in today's information environment. Access to computers, growing levels of expertise, and a growing realization of the power of Internet makes CNO a difficult challenge. CNO falls into three categories: Computer Network Attack (CNA), Computer Network Defense (CND) and Computer Network Exploitation (CNE).[16]

- **Computer Network Attack (CNA).** The role of the Internet and computers is increasing even in military operations. The use of the Internet by adversaries to communicate, to gain information, or to disseminate propaganda, misinformation, and disinformation is common. The international role and legal considerations make CNA a strategic issue but with operational impacts. Although classification issues are always a concern; the ability to conduct offensive operations on the Internet is a fact and it is one that requires careful

consideration prior to its employment. Modern industries utilize Supervisory Control and Data Acquisition (SCADA) systems to monitor and control communication and industrial networks. Although SCADA improves efficiency it also provides vulnerability via computers to disrupt commercial ventures. The ability to attack SCADA systems allows the disruption of communication infrastructure, power grids, and various industrial efforts. Offensive computer operations against these types of system could potentially disrupt an adversary's infrastructure enhancing effectiveness of military operations.

Although there was no proof of Russian government backing, the cyber attacks or distributed denial of service (DDOS) on the Estonian private banking and media networks in 2007 caused the Estonian government to "shut down key computer systems for their own protection."[17] The cyber attack temporarily disrupted the Estonian government's computer usage and sent a clear demonstration to the world of the potential impact of offensive computer capabilities. The 2008 Russian incursion into Georgia was also preceded by a cyber attack, once again lacking proof of Russian government backing that effectively resulted in a temporary denial of access to Georgian government websites. This action prevented the Georgian government from spreading "its message online and to connect with sympathizers around the world."[18] Both these instances were against countries whose reliance on the Internet and computers was still growing. Such a cyber effort against a more developed cyber nation could have international impact.

In regards to military operations, the ability to attack networks must be taken into planning considerations even though the expertise to conduct such operations is under strategic control. Too often, requests to remove specific Internet sites in order to prevent information dissemination or to stop propaganda are done without thought to legal or intelligence gathering considerations. The IO officer is not the subject matter expert on computer operations but should serve as the primary point of contact with strategic elements that serve as the executors for such operations. The second and third order of effects must be taken into consideration and the strategic impact should be balanced with the operational or tactical gains.

- **Computer Network Defense (CND).** The protection of the military's network is critical to its communication infrastructure. The Congressional Clinger-Cohen Act of 1996 and the U.S. Presidential Decision Directive 63 provide guidance to departments to "ensure that the information security policies, procedures, and practices of the executive agency are adequate" and that threats to the information infrastructure are addressed.[19] The military's use of computers and the Internet require a robust information assurance program to protect its information infrastructure. Establishment of antivirus, fire walls, computer assurance training programs, and other efforts help protect the network. The military's implementation of numerous protection programs receives command emphasis, but just like IO it receives the most attention when there is a failure in the protection. CND's relationship to OPSEC cannot be denied especially in a world of personal websites such as 'Facebook',

blogs, and a readily available hacking technology.

- **Computer Network Exploitation (CNE).** The exploitation of computers is a growing information/intelligence gathering capability that has not yet reached its potential. An ever increasing use of the Internet and computer related activities provide a rich environment to gather intelligence on communication and activities. Just as in CNA and CND, the expertise requirement for exploitation is normally not found at the tactical or operational levels but its impact can be felt there. Legal considerations and technology requirements require strategic resources. The international growth of Internet has provided instantaneous information dissemination and acquisition but friendly and adversarial forces are both utilizing this resource. Just as raw intelligence, CNE requires assessment and analysis to fully develop a useful picture. IO involvement in CNE, just as in CNA and CND, is one of integration. Serving as a target nomination capability, IO efforts also relay the requirements of the commander to those agencies with the resources to execute.

Electronic Warfare (EW). Joint Publication 3.0 defines that EW involves "the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[20] EW is not new to the military but recent events in Iraq and Afghanistan has seen a resurgence in this effort. Currently the EW effort in Iraq focuses on the Improvised Explosive Device (IED) threat but its ability to disrupt communication provides an invaluable resource when attempting to disrupt an adversary's decision-making cycle. The U.S. Army's revitalization of EW is a clear demonstration of its importance in today's communication environment. "All of the core, supporting and

related IO capabilities either directly use EW or indirectly benefit from EW."[21] With increased reliance on wireless communication and the growing popularity of IEDs by terrorists, EW's role in the tactical fight is increasing. EW capabilities, normally maintained at the strategic or operational levels are being utilized in support of the tactical fight. Responses to media queries but more importantly the impact that EW may have on both military and civilian operations requires a close coordination of public affairs with those involved in CMO. Utilization of EW to disrupt an adversary's command and control adds another invaluable tool in the IO practitioner's arsenal. This means it is even more important to deconflict and synchronize EW to prevent information fratricide or to prevent desynchronizing the overall IO effort.

Operations Security (OPSEC). Joint IO doctrine states that "OPSEC denies the adversary the information needed to correctly assess friendly capabilities and intentions."[22] Normally OPSEC is not a concern unless there is an issue. Modern technology in the form of blogs, wireless communications, and media embeds make OPSEC all the more important to prevent the inadvertent release of potentially damaging information. Taking into consideration all the capabilities of IO, OPSEC serves as a simple protection means but one that is often overlooked. Simple common sense rules apply but it requires a resource whose primary mission is to protect unclassified information. During III (US) Corps' 2006-2008 Iraqi rotation much of their success in the area of OPSEC was due to command emphasis and the dedication of manpower resources, whose only mission was to establish OPSEC procedures, maintain oversight and administer training programs for subordinate commands. [23]

OPSEC is a frame of mind that requires constant attention, just as safety does. OPSEC programs are common throughout the various services and training is available but normally responsibility is assigned as an additional duty. Under the Army's new modular construct, the OPSEC officer is part of the protection cell but its duties include areas that expand past simple protection. Military news releases, service member posting on the Internet of pictures and correspondence, command information programs, and unit trends all present a picture to potential adversaries. The challenge of OPSEC is not the release of classified information but rather pieces of a puzzle that provides adversaries with a picture of the overall operation. Just as IO integrates the other information efforts, the OPSEC portion of IO must be integrated into all facets of military operations to begin with the planning.

Military Deception (*MILDEC).* The use of MILDEC is possibly one of the most underutilized and misunderstood elements of IO. JP 3-13 states "MILDEC seeks to encourage incorrect analysis, causing the adversary to arrive at specific false deductions."[24] The basic principle of MILDEC requires a believable and feasible foundation to be successful and it is the various tools of IO that help establish feasibility. Deception infers falsehood, but that is not the case; however, it does require careful planning and information control. The hesitancy to utilize MILDEC relates to its need to be feasible and the resources required in facilitating success. The challenge is to dedicate resources to support the MILDEC without jeopardizing other operations and that requires commander guidance. A major risk when using information venues to support MILDEC is the loss of credibility; such a risk should not be taken lightly nor is it a requirement to jeopardize credibility to effectively support MILDEC. The use of

OPSEC is extremely important when dealing with MILDEC, not to inform but to deny information. What provides credibility is presentation of word and deed but the most powerful resource is to present a truthful picture that supports the MILDEC.

Normally the most successful MILDEC operations provide a truthful picture, but putting various pictures together presents the adversary with a vision that is inaccurate. Military history is filled with examples of deception; it is not a necessary ingredient to military success but it serves as a multiplier. Planners must assess military deception during the initial phases of planning to see if the risk and required resources are cost beneficial. In the current information environment exposure of an attempted deception is always a risk and access to vast amounts of information increases the risk of exposure. The second and third order of effects for exposure must be taken into consideration and plans must include how to react to exposure and how to mitigate it. The common theme, just as with all the other core IO capabilities, is integration.

Information Operations Related Elements

Public Affairs (PA). The task of PA is to inform all audiences of information that may be pertinent regarding the military and its operations. PA aids the IO effort by providing information to media and friendly audiences that help present the U.S. and specifically the military perspective. PA helps highlight military successes, counter misconceptions and counter false adversarial propaganda. IO and PA should compliment each other in their effort to tell the military's story and shape the information environment. The development of messages and themes to support military operations should include PA to ensure that the proper and truthful messages are reaching all audiences. Part of this integration is continuity in the messaging. If media reporting

counters the messages delivered by the military then credibility is at risk. Challenges regarding PA and IO have surfaced, not in the act of informing but rather in their working relationship and their respective roles. The example cited earlier in the PSYOP portion of this document, regarding paid media, demonstrates how even factual information can be seen as tainted.

The use of PA to counter misinformation or disinformation is vital but the PA messaging and the rest of IO communication venues such as PSYOP or IE must be consistent to ensure maintaining credibility. The military's PA structure is a major supporter of the overall strategic communication effort and provides the military with the means to inform the U.S. populace and neutral audiences. IO should provide the necessary support to the PA because although it is the mission of PA to inform, it is the information released by PA that in truth may influence. PA must be cognizant of what operations are on going and what messages are being disseminated by the other capabilities. The use of a communication working group as a technique to synchronize information efforts has proven successful. This technique does nothing more than serve as a means to integrate the information effort. PA and IO capabilities should not be competitors but rather mutually supporting in their efforts. The ability to inform with the truth is at times a most powerful weapon in the fight for information superiority.

Civil Affairs (CA). CA serves as a useful tool supporting IO in both deed and word. The actions of CMO provide some of the deeds that show the military's intent and provide the other elements, such as PA, the ability to show the actions through words. The interaction between the organizations that conduct the CMO and the other players such as non-governmental and governmental organizations, serves as a key

player in the IE process. The information acquired through routine CMO is instrumental in the identification of key audiences and conduit audiences. The routine engagements of those involved with CMO can be instrumental in the overall IE process. CMO daily interaction and the actions resulting from CMO are influential and nonsynchronization with the overall effort can be disastrous. Although not directly supporting IO, CMO can benefit from IO efforts. CMO units, aware and supporting the various commander's objectives, help the "speaking with one voice" process. To often CMO acts independently or parallel with IO and PA; this is a staffing challenge. The integration of the three provides an enhanced messaging capability. CMO's ability to also provide feedback to other IO efforts, specifically PSYOP, can also enhance effectiveness measurement. The benefits of a cooperative effort provide exposure of the good deeds done by Civil Affairs units.

Information Operations Enablers

Strategic Communication. Although strategic communication is not a military specific capability, the impact of strategic communications is felt at all levels of military operations. Information serves as a multiplier that gives credibility to "words, images, and actions" but information without the support of actions is merely words of no consequence[25]. Strategic communication is one of the primary weapons to battle misinformation and disinformation at the strategic level. IO, the military arm of the national information effort, supports strategic communication and public diplomacy through its actions and supporting information efforts. If the strategic communication and the military themes are contradictory then credibility is lost.

It is said that the purpose of strategic communications is to “provide audiences with truthful and timely information that will influence them to support the objectives of the communicator.[26] Many times the communicator is the military, be it in a combat or peaceful environment. Combatant Commanders routinely conduct military operations in the form of military exchanges, humanitarian missions, or routine military operations. Military organizations must know the strategic communication objectives and support our national effort. Recent initiatives to improve the coordination between the military and the State Department should also result in an improved communication effort. Since strategic communication influences all audiences, the messaging is of particular interest to the military.

In July of 2006, then U.S. Representative Newt Gingrich criticized the State Department's "inability to manage the information campaign advocating U.S. foreign policy interests"[27] adding to a long list of criticisms for a perceived failure of strategic communication. Accusations of legal impropriety by conducting psychological operations against the American populace, unethical placement of media products to mislead foreign audiences, unsynchronized and ineffective messaging and a lack of credibility in message dissemination are common criticisms. Just as IO is responsible for integration for the employment of its capabilities, the national government must improve the employment and synchronization of strategic communication and the military's role to support it. The State Department’s 2007 *National Strategy for Public Diplomacy and Strategic Communication* helps shape how the national government and its military can "compete against propaganda and tell its story."[28] Strategic

Communication success can positively impact what is referred to as the "IO War" and achieve information superiority in the information environment.

Information Engagement (IE). Although not a core element of IO, IE has gained prominence since the development of strategic communication and the growing impact that media has on the information environment. U.S. Army publications state that IE is "the integrated employment of public affairs to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and, leader and Soldier engagements to support both efforts."[29] It is a concern that the Army's new Field Manual (FM) 3-13, may reinforce this perception that IE will replace IO in its description of the G7 and information tasks (see figure 3).

During Kosovo Forces operations in the Balkans, one of the primary means of engagements was the daily face-to-face interaction between Soldiers and the local populace. Key leader engagements were planned and executed with a desired end state to achieve specific effects. IE occurs at various levels and throughout the military structure; the orchestration of messages and themes aids in the "speaking with one voice". It is an implied task for the IO officer to plan and orchestrate IE for the Commander, but the execution is delegated to a wide variety of action organizations. Key leaders, Soldiers, PA, PSYOP, CA, and others are all potential means to execute IE.

Task	Information Engagement	Command and Control Warfare	Information Protection	Operations Security	Military Deception
Intended Effects	•Inform and educate internal and external publics •Influence the behavior of target audiences	•Degrade, disrupt, destroy, and exploit enemy command and control	•Protect friendly computer networks and communication means	•Deny vital intelligence on friendly forces to hostile collection	•Confuse enemy decision-makers
Capabilities	•Leader and Soldier engagement •Public affairs •Psychological operations •Combat camera •Strategic Communication and Defense Support to Public Diplomacy	•Physical attack •Electronic attack •Electronic warfare support •Computer network attack •Computer network exploitation	•Information assurance •Computer network defense •Electronic protection	•Operations security •Physical security •Counterintel-ligence	•Military deception

Figure 3. Information Tasks[30]

IE's role in the overall IO process focuses on the effort to inform. The integration of the information task of informing and the other roles of IO, such as disrupting or influencing, remains the IO officer's primary role. As always, consistency of messages is key. Just as consistency is important so is the orchestration of the engagements. Identification of who the key audiences are, what the proper message should relate, and ensuring consistency require a dedicated resource but care should be taken not to replace IO with IE.

Information Operations Doctrine. IO doctrine has been an evolving progression. Although the basics of IO have always been involved in military operations in one form or another, its introduction into formal doctrine has given it structure. With this doctrinal structure also comes the development of an IO career force. The U.S. Army's implementation of the functional area (FA) 30 (the Army IO officer) was the first step.

Other services have implemented IO officers with special training in addition to their primary career path. Most services focus on the more technical aspects of IO and accordingly most of the selected IO officers come from technical backgrounds. Complimentary fields such as intelligence, PSYOP, and combat arms fields have also found their way into the IO career field.

The U.S. Army introduced its initial IO doctrine in the form of FM 100-6 in August of 1999. FM 100-6 defined IO as "continuous military operations within the Military Information Environment that enable, enhance and protect the friendly force's ability to collect, process and act on information to achieve an advantage across the full range of military operations. IO includes interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities."[31] The Balkans served as a testing ground for the doctrine to include maturity of various TTPs. The Army's Land Information Warfare Activity (LIWA) provided Field Support Teams (FST) to deployed units while continuing to develop IO and its doctrine. It was the duty of the FST to provide U.S. forces with the expertise and some additional manning resources to employ this new concept. Normally FSTs worked directly for the S3 or Commander and served as special staff but their training consisted of internal training programs provided by LIWA as part of their pre-deployment preparation. Later specialty schools or courses such as MILDEC, EW and OPSEC were incorporated into the training programs. The five person FSTs were not adequate enough to fully employ IO so commanders began to dedicate resources in the form of Fire Support personnel to serve as IO officers at the subordinate commands. Commanders in Bosnia and Kosovo began to understand the importance of IO, but their environment focused on the non-

technical aspects of IO based on adversaries and audiences. The five elements of Command and Control Warfare were combined under IO into one integrated approach to better synchronize its efforts.[32] Although the focus of IO in the Balkans was PA, PSYOP and face-to-face engagements, the more technical aspects of IO continued to develop doctrinally.

Training and Manning Structure. Training and manning is a critical enabler for IO within the military and civilian information structures. The current information environment requires a coordinated effort, which begins with training and manning, between military and inter-agency organizations to ensure an integrated message delivery and common employment of IO and its capabilities.

- **Training.** The IO Roadmap, published by DoD in 2003, played "a significant role in shaping how DoD, the Services and Combatant Commanders organize, train, equip, plan and execute information operations."[33] The development of a trained IO career force is more important now as the power of information is being employed at all levels. Although the Joint community has developed some general formal IO training programs only the Army currently has a functional area that is specifically focused on IO.

  Services focus their internal IO training programs on their respective requirements for IO. The natural tendency of the Services is to focus on those areas of IO that best serves their specific mission requirements. While some focus on the more technical elements others focus on the more human influence capabilities such as PSYOP, CMO, IE or PA. The Roadmap described a solution that "includes the development of a core cadre of

professionals capable of planning and executing fully integrated IO."[34] The key is full integration of IO, not only the technical aspects, the PSYOP, the IE, or the communications portion. The various Services and more importantly the Joint training programs must focus on the holistic employment of IO. The IO officer should have a working knowledge of all the elements of IO; it is the IO officer's purpose to integrate and synchronize the information effort. The IO training programs must focus on the integration process, providing the IO officers with the knowledge to best employ all forms of IO. The IO officer should not be seen as the expert for all the various elements but rather as the coordinator.

The various service schools' IO curriculums seem to provide leaders and staff officers with the basic fundamentals of IO, and the Joint IO programs sufficiently provide those skills required to plan and integrate IO into Joint operations. IO officers also have the opportunity to gain additional expertise in specific areas such as MILDEC, OPSEC, and Special Technical Operations. These types of augmentation training in addition to advance schooling opportunities provide additional skills to the general IO planning and coordination capabilities. Training standardization and interoperability must be improved. Recent comments regarding the Army's FA 30 Qualification Course is that the course's focus is not on the general IO concept but rather on IE. The IO Roadmap provided several recommendations on how to improve IO to include the assertion that "programs of instruction for joint IO planners and specialists must be

standardized."[35] The growth of IO within the military and the information effort at the national level clearly demonstrate the need of a trained and capable IO career field.

- **Manning**. The Army predominantly provides IO support to current operations in Afghanistan and Iraq but other service support is increasing. The USMC's expansion into the IO career field and the support through the core elements by all the services is truly making IO a joint program. On the joint staff, the IO officer assumes the position as the J39 under the Operations section or J3. The Army IO staff officer serves as special staff as the G7 but none of the Services have yet developed an enlisted IO career field. In support of Operation Iraqi Freedom and Operation Enduring Freedom, various staffs IO positions are filled by all the services, IO requirements dictated by the Joint Manning Documents (JMD). These requirements stipulate IO training but frequently officers receive rudimentary IO training enroute to the assignment. The use of Intelligence or signal officers is not uncommon. Although the Army attempts to meet JMD IO requirements with FA30s, the availability of experienced and trained officers is not always present.

The growing popularity of the effects concept also saw the rise and implementation of an effects element. These effects elements varied between the commands and were primarily personality driven. An example of this was within Multinational Corps Iraq where the Effects Division was responsible for Engagements, IO, EW, Assessments, and other

organizations. EW's separation from the IO section was primarily due to the specific role that EW had in the IED fight. PSYOP, OPSEC and MILDEC remained under IO supervision. Although EW and Engagements were not under the IO control, the IO staff still had the responsibility to coordinate efforts through the Effects Coordinator.

Just as important as it is for training to be standardized so is the use of the IO staff. Special staff or within the operations staff, the physical location of the IO organization is not the issue but the method of staff integration is important. The process of IO into the operational effort is critical so many argue that the IO organization should be embedded in the operations staff. Others are under the belief that IO as a special staff will enhance command emphasis and provide the flexibility to focus only on information tasks. What the services and the Joint community must address is a standardization of the specific duties of the IO officer. Additional studies are needed to assess the various IO staffs, their manning, and their placement within the many staff organizations.

Measures of Effectiveness (MoE) /Measures of Performance (MoP). The development of MoEs and supporting MoPs has always been a challenge. Unfortunately development of MoEs and MoPs sometimes occurs after the planning effort is complete and another challenge is how to brief it! MoEs are difficult to quantify at times since they are used to "assess changes in system behavior, capability, or operational environment"[36] but frequently MoPs are confused for MoEs. Effects Based Operations (EBO) brought additional attention to the importance of MoEs and MoPs but

with that came confusion of what MoEs are and why they are important. The challenge comes in how to quantitatively display that an effect has been achieved. MoEs and MoPs are success or failure indicators. They help provide the picture, an assessment of the operation or environment. Individually IO capabilities have their own measures but integrating them into a complete assessment of effectiveness will provide the commander a better view of the objective's progress. The information acquired through local observation and dialogue can provide an assessment of other efforts and the needs/desires of target audiences. The combination of technical, PSYOP, CMO and other capability assessments can provide a more thorough perspective than a single poll or news reports.

Recommendations

The military's supporting role to the national government's objective to achieve information superiority is generally a success, but it can be improved. The following six recommendations, based on personal observations and experiences, would address many of the IO challenges facing U.S. military and civilian leadership.

1. The military IO career path must focus its efforts on preparing the IO officer to be familiar with all facets of the information tasks and on integrating these tasks to achieve information superiority.
2. Doctrine must be expanded to include improved methods of supporting the strategic communication effort without removing the technical aspects of IO.
3. IO officers in each of the services must be interchangeable; standardization in training and employment is key. As has been outlined in the IO Roadmap, "instruction for joint IO planners and specialists must be standardized"[37] but

the current program's effectiveness is in question. Although each service defines its own priority requirements for their organic IO professions, the basic foundation of training should be comparable.

4. In regards to a professional IO career force, serious consideration should be taken to add an enlisted branch to the IO career path. Augmenting the IO staff with enlisted personnel or warrant officers, trained in areas such as computer operations, communications, military intelligence, operations, or electronic warfare will add depth and expertise.
5. Changing current perceptions regarding IO and its employment is a task that must be undertaken by U.S. military and civilian agencies alike. Changing the perception of the proper employment of information power is an area that is beyond the scope of military control, but within its realm of influence. This requires attention at the national level; reconsideration of implementing a national information strategy office or similar capability is needed if we are truly going to achieve information strategy. Perception change requires addressing ethical and legal concerns on the ability to “market” the messages to friendly audiences. We must level the playing field in an effort to counter propaganda. "*The National Strategy for Public Diplomacy and Strategic Communication* is a positive step in permitting the United States to compete against propaganda and proactively tell its story."[38] The U.S. military and civilian information agencies must agree to a common understanding of IO, what its capabilities are and jointly address the points of confusion. The concept that "changing perceptions, attitudes, and untimely beliefs is a generational endeavor"[39] is true.

6. Efforts to improve coordination between interagency and the military must include a more synchronized information effort. Implementing common themes, standardized training, employment techniques, and doctrine will aid the synchronization effort.

Conclusion

Achieving an operational advantage in regards to the information environment is feasible but in the modern information environment complete and constant dominance is not. IO cannot solve all U.S. information woes, but it can synchronize our efforts and present our audiences with a cohesive and effective communication tool. With all the various capabilities available to the U.S. in its efforts to gain superiority, efforts must remain focused and integrated at all levels, especially the national level. The use of IO as an integration process within the military structure is paramount. Just as a home is built using plumbers, electricians, carpenters, and masons working according to an integrated plan, IO must focus on the overall project, not a single piece of it. The perception that one particular capability or event can solve our problems is misleading. It is a continuous effort; there will be periods of success and periods of failure. We must be poised to take advantage of the successes, while remaining ready to mitigate or correct apparent failures.

Endnotes

[1] U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington DC: U.S. Joint Chiefs of Staff, February 13, 2006), GL9.

[2] Ibid., ix.

[3] "III (US) CORPS Information Operations Iraq Rotation 06-08 Briefing" (February 2008)

[4] George Bush, *The National Security Strategy of the United States of America.* (Washington, DC: The White House, March 2006), 11.

[5] Dennis Murphy and James White, "Propaganda: Can a Word Decide a War?," *Parameters* 37, no. 3 (Autumn 2007), 17.

[6] Edward Coffman, *The War to End all Wars*, (Lexington: The University Press of Kentucky, 1998), 191-192.

[7] U.S. Joint Chiefs of Staff, *Information Operations*, I-9 - I-10.

[8] Author's compilation of definitions from various Joint and Army publications.

[9] U.S. Department of Defense, *Irregular Warfare (IW)*, DoD Directive 3000.07 (Washington DC: U.S. Department of Defense, December 1, 2008), 8.

[10] U.S. Joint Chiefs of Staff, *Information Operations*, 1-6.

[11] Brian McKiernan, "IO Roadmap: One Right Turn and We're There," In *Information as Power, Volume 2*, ed. Jeffrey L. Groh, et al. (Carlisle Barracks, PA: U.S. Army War College, 2007), 23.

[12] U.S. Joint Chiefs of Staff, *Information Operations*, GL-11.

[13] Murphy, "Propaganda: Can a Word Decide a War?," 22.

[14] U.S. Joint Chiefs of Staff, *Information Operations*, II-2.

[15] Borzou Daragahi and Mark Mazzetti, "U.S. Military Covertly Pays to Run Stories in Iraqi Press," *Los Angeles Times*, November 30, 2005, http://articles.latimes.com/2005/nov/30/ world/fg-infowar30 (accessed January 19, 2009).

[16] U.S. Joint Chiefs of Staff, *Information Operations*, II-5.

[17] Larry Greenemeier, "Estonian Attacks Raise Concern over Cyber 'Nuclear Winter'," May 24, 2007, *Information Week*, http//www.informationweek.com/news/internet/ showArticle.jhtml?articleID=199701774 (accessed November 16, 2008).

[18] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?partner=rssnyt (accessed January 20, 2009).

[19] LaWarren V. Patterson, *Information Operations and Asymmetric Warfare... Are We Ready?,* Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, April 9, 2002), 4.

[20] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington D.C.; U.S. Joint Chiefs of Staff, September 17, 2006, Change 1, February 13, 2008), GL-12.

[21] U.S. Joint Chiefs of Staff, *Information Operations*, II-4.

[22] Ibid., II-2.

[23] Based on personal observations from author and input to the III (US) CORPS internal after action report for OIF Rotation 06-08, February 2008.

[24] U.S. Joint Chiefs of Staff, *Information Operations*, II-2.

[25] Dennis Murphy, "Strategic Communication Wielding the Information Element of Power," In *U.S. Army War College Guide to National Security Issues, Volume 1: Theory of War and Strategy* (Carlisle Barracks, PA: U.S. Army War College, June 2008), 180.

[26] James Stavridis, "Strategic Communication and National Security", *JFQ*, no. 46 (3rd Quarter 2007), 4.

[27] Khody Akhavi, "The Media War", *Political Research Associates: Right Web*, http://rightweb.irc-online.org/rw/4342.html (accessed November 1, 2008).

[28] Murphy, "Propaganda: Can a Word Decide a War?," 26.

[29] U.S. Department of the Army, *Operations*, Field Manual 3-0, (Washington DC: US Department of the Army, February 27, 2008), 7-3.

[30] Ibid.

[31] Center for Army Lessons Learned, *Information Operations*, Newsletter, 99-2 Newsletter (January 1999),1.

[32] Ibid., 2.

[33] McKiernan, "IO Roadmap: One Right Turn and We're There," 5.

[34] Ibid., 13.

[35] Ibid.

[36] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, GL 17.

[37] McKiernan, "IO Roadmap: One Right Turn and We're There," 13.

[38] Murphy, "Propaganda: Can a Word Decide a War?," 26.

[39] Ibid.